14920

Putnam, Robin (SCA)

From: noreply@formstack.com
Sent: Wednesday, April 10, 2019 10:58 PM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications

Formstack Submission For: Security Breach Notifications - With Addresses

Submitted at 04/10/19 10:57 PM

Business Name:	H. CARSON SMITH, IV, P.C.
Is the business located in the United States?:	Yes
Business Address:	4474 Commerce Dr. Buford, GA 30518
Foreign Business Address:	
Company Type:	Other
Your Name:	Colin Battersby
Title:	Counsel
Contact Address:	McDonald Hopkins, PLC 39533 Woodward Ave., Ste. 318 Bloomfield Hills, MI 48304
Contact Address:	
Telephone Number:	(248) 593-2952
Extension:	

RP

Email Address:	cbattersby@mcdonaldhopkins.com
Relationship to Org:	Other
Breach Type:	Electronic
Date Breach was Discovered:	03/06/2019
Number of Massachusetts Residents Affected:	1
Person responsible for data breach.:	Unknown
Please give a detailed explanation of how the data breach occurred.:	H. Carson Smith, IV, P.C. recently learned that on October 2, 2018, an unauthorized individual may have obtained access to a firm email account. H. Carson Smith, IV, P.C. immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the email account and the security of the emails and attachments contained within it. H. Carson Smith, IV, P.C. devoted considerable time and effort to determine what information was contained in the affected email account. Based on its comprehensive investigation and document review, which concluded on March 6, 2019, H. Carson Smith, IV, P.C. discovered that the compromised email account contained a limited amount of the affected resident's personal information.
Please select the type of personal information that was included in the breached data.:	Social Security numbers = Selection(s) Driver's License = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach was a result of a malicious/criminal act. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information	Yes

was restricted to authorized personnel only.:	
Network configuration of breached system:	Internet Access Available
For breaches involving electronic systems, complete the following:	Personal information stored on the breached system was password-protected and/or restricted by user permissions. = Selection(s)
Does your business maintain a Written Information Security Program (WISP)?:	Yes
All Massachusetts residents affected by the breach have been notified of the breach.:	Yes
Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::	Option2 | US Mail
Please explain your answer of Other Above:	
Date notices were first sent to Massachusetts residents (MM/DD/YYYY):	04/10/2019
All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services.:	Yes
If the breach of security includes a Social Security number, Massachusetts law requires your credit monitoring comply with Section 3A of Chapter 93H:	I acknowledge our credit monitoring complies with section 3A of Chapter 93H
Law enforcement has been notified of this data breach.:	No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring, including updating your WISP.:	H. Carson Smith, IV, P.C. launched a thorough investigation and provided the affected resident with written notification of this incident and offered a complimentary one-year membership with a credit monitoring service. At H. Carson Smith, IV, P.C, protecting the privacy of personal information is a top priority. H. Carson Smith, IV, P.C. is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. H. Carson Smith, IV, P.C. continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information. H. Carson Smith, IV P.C. changed the password on the affected account as a result of this incident.
Yes / No:	Yes
File 1 Upload:	View File
File 2 Upload:	
File 3 Upload:	
File - 4 Upload:	

Formstack, 11671 Lantern Road, Suite 300, Fishers, IN 46038

14920

H. CARSON SMITH, IV, P.C.
ATTORNEY AT LAW
4474 COMMERCE DRIVE, SUITE B
BUFORD, GA 30518
P.O. BOX 606, BUFORD, GA 30515

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

[redacted]

Dear [redacted]

I am writing with important information regarding a recent security incident. The privacy and security of the personal information we maintain is of the utmost importance to H. Carson Smith, IV, P.C. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

We recently learned that an unauthorized individual may have obtained access to a limited amount of your personal information, including your full name, Social Security number and driver's license number.

To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well. To protect you from potential misuse of your information, we are offering you a twelve-month membership in myTrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion. For more information on identity theft prevention and myTrueIdentity, including instructions on how to activate your twelve-month membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 AM to 8:00 PM CST.

Sincerely,

[redacted]

H. Carson Smith, IV

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

You can sign up for the online credit monitoring service anytime between now and [redacted] Due to privacy laws, we cannot register you directly. Please note that credit monitoring service might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you believe you may be a victim of identity theft, please call the toll-free TransUnion Fraud Response Services hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] to speak to a TransUnion representative about your identity theft issue.

2. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Obtaining a Police Report.

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.